STRATEGY RESEARCH PROJECT

GENERAL! THEY'VE CAPTURED OUR HARD DRIVE!

BY

COMMANDER MARK NAULT
United States Navy

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGIC RESEARCH PROJECT (SRP)

GENERAL! THEY'VE CAPTURED OUR HARD DRIVE!

by

CDR Mark Nault, USN

COL Robert Coon, USA (Retired)
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: CDR Mark Nault, USN

TITLE: General! They've Captured Our Hard Drive!

FORMAT: Strategy Research Project

DATE: 2 November 1997 PAGES: 34 CLASSIFICATION: Unclassified

Joint Vision 2010 (JV 2010), an overview document describing the strategic vision of the Chairman of the Joint Chiefs of Staff (CJCS), was released in early 1997 and revealed a new joint armed forces battlespace concept called Full Spectrum Dominance (FULL SPECTRUM DOMINANCE). Information Operations (IO), which includes both Information Warfare (IW) and Command and Control (C2) doctrine, is the backbone of this emerging JV 2010 FULL SPECTRUM DOMINANCE concept. Are there any significant strategic level IO concerns, for our military leaders who practice the strategic art in today's and tomorrow's joint armed forces, which ultimately delay or degrade the capabilities detailed in the new JV 2010? This author believes that the answer to this thesis question is a resounding YES!

This Strategic Research Project (SRP) briefly reviews several basic, but recently updated, IO definitions, and describes the role that IO plays in the cyber-missions depicted in the new JV 2010 and other related documents, such as the President's National Security Strategy (NSS), the Quadrennial Defense Review (QDR), the CJCS's National Military Strategy (NMS), as well as individual service concept documents. Furthermore, this SRP brings to light several key issues, which have the potential to negatively impact the total package, previously referred to as Full Spectrum Dominance. Several recommendations are also included, as food for thought for those who are now, or soon will be working hard in the strategic joint arena.

TABLE OF CONTENTS

PREFACE

This Strategic Research Project (SRP) was prepared for two reasons. First, the United States Army War College (USAWC) requires that the written results of each student's research on a topic of choice be submitted for approval prior to graduation. The SRP topic is required to be addressed at the strategic level, in a paper containing not less than 4500 words, but not to exceed 6000 words (exclusive of endnotes and bibliography). This paper meets these requirements.

Second, this essay was an attempt to spotlight several strategic issues and concerns, focusing on the blossoming realm of Information Operations (IO). Each highlighted area has been described and analyzed, revealing conclusions on the potential impact on current and future military strategy. This author's hope is that these research results may provide some food for thought for current and future practitioners of the strategic art.

This author would like to thank COL Bob Coon, US Army (Retired), for his assistance as Project Advisor during the research and writing phases of this SRP, as well as for his wit and humor during its creation. Special thanks also go to Professor Bob Minehart, USAWC, for his technical help, especially during the preliminary research struggle. Also, thanks go to this author's USAWC Core Course Faculty Instructors for their help in laying the strategic foundation for this SRP. These gentlemen are COL Paul Cunningham, USAR, Professor Bill Rodier, CIA, and COL Jay Lawson, USA. Finally, this author personally and deeply thanks the members of USAWC Class of 1998, Seminar 15, "The Strategic Paws", for making the entire Army War College experience a truly memorable one. Go Paws!

> A paradox of modern battlefield technology is that an intelligence analyst in Washington D.C., often knows better than the infantryman what lies beyond the next hill. The challenge is to fuse that knowledge with the data collected from other sources, preserve security and still get the product into the hands of the soldier before he must solve the mystery himself - the hard way.
>
> — Alan D. Campen

THESIS - STRATEGIC CONCERNS WITH THE VISION

Joint Vision 2010 (JV 2010), an overview document describing the strategic vision of the Chairman of the Joint Chiefs of Staff (CJCS), was published in early 1997 and revealed a new joint armed forces concept called Full Spectrum Dominance. Information Operations (IO), which includes both Information Warfare (IW) and various Command and Control (C2) doctrine, is the backbone of this emerging JV 2010 concept, and is highlighted in the opening quotation of this paper. This author's research in this arena has resulted in several significant strategic level IO, IW, and C2 concerns, which may delay or degrade the FULL SPECTRUM DOMINANCE capabilities detailed in the Chairman's new JV 2010. The bottom line is that unless BIG CHANGES are MADE SOON, WE WON'T MAKE IT ON TIME!

This essay will discuss the ingredients of the current Full Spectrum Dominance concept, and will present each of the several significant IO issues, which challenge the full realization of JV

2010 goals. Finally, a few recommendations will be provided, not as "silver bullets", but as catalysts for deeper strategic thinking. These thoughts are submitted in the hope that military leaders, who will practice the strategic art in today's and tomorrow's joint armed forces, will be better armed in their charge up the Full Spectrum Dominance hill of future military operations. The goals of every strategic leader should include preventing soldiers from having to find out about the enemy over the next hill "the hard way".

THE ROADMAP TO SUCCESS

The opening statements of this paper, have just presented a brief and clear strategic level thesis. The roadmap that this paper will follow, will next set the stage for later detailed issue analysis, with a description of Full Spectrum Dominance, Information Operations, and several related concepts, as described by current military doctrinal publications. Further down the road, the reader will find a description and a discussion of two categories of IO concerns. These concern categories are Political/Cultural and Technical/Practical. Examples of specific concerns in each category will then be presented and discussed, to help solidify the characteristics and features of each area of concern.

Immediately following all this bad news, will be some good news. This good news section will highlight a few military activities which are directly contributing to the potential success of the JV 2010 mission. Finally, the roadmap reveals the ultimate destination, which contains a summary and several recommendations for changes, which if debated and instituted soon, might just get us back on the road to JV 2010 success. The overall goal of this final section is to provide the rest of the story, which is unfortunately omitted from Joint Vision 2010, and the other high level strategy "glossies". This will hopefully provide some food for thought for strategic leaders, who would prefer to be "better armed" than "blissfully deficient", in the high speed world of computerized information technology.

STARTING WITH A FULL DECK!

> It is not enough to try just to think systematically. If the right information is not available - or, more likely, it is incomplete - the final analysis, no matter how well one has thought, will be seriously flawed. You must start with a full deck.
>
> — John L. Petersen

This section will help ensure that the reader has "a full deck", with respect to current Full Spectrum and Information Operations (IO) doctrine, by highlighting the four major Full

Spectrum Dominance components, and by providing a brief description of a few key IO concepts. First, the CJCS's main JV 2010 themes will be reviewed. In the opening paragraphs of Joint Vision 2010, General Shalikashvili states that, "This vision of future warfighting [Full Spectrum Dominance] embodies the improved intelligence and command and control available in the information age and goes on to develop four operational concepts: dominant maneuver, precision engagement, full dimensional protection, and focused logistics...Together, the application of these four concepts by robust high quality forces will provide America with the capability to dominate an opponent across the range of military operations."[1]

The Full Spectrum Dominance component of Dominant Maneuver involves the combined effects of dispersed, synchronized forces with the speed and accuracy of massed effects to apply decisive force. Precision Engagement ties intelligence and command and control together to allow greater capability to shape the battlespace. A third Full Spectrum Dominance concept, Full Dimensional Protection, keys on the multi-layered approach, including improved sensors and continuous unit identification. Finally, Focused Logistics blends improved in-transit visibility, with transportation means flexibility and tailoring, to maximize the effects of the other three pieces of the Full Spectrum Dominance pie. The "crust" of the pie is battlespace information superiority through technological innovations, which are hoped to be developed between now and the year 2010.

The continuously evolving world of Information Operations itself will now be discussed. On 9 December, 1996, the Secretary of Defense (SecDef) promulgated classified directive S3600.1, titled Information Operations. This document provided updated definitions, policy, and responsibilities for military Information Operations, including various aspects of Information Warfare. An unclassified excerpt defines military Information Operations (IO) as, "Actions taken to affect adversary information and information systems while defending one's own information and information systems".[2] This is a broad, sweeping concept, and IO is often better described by some of its subsets.

Another concept, Information warfare (IW), is one subset of the all inclusive concept of Information Operations, and is defined as, "IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries".[3] IW, then, can be described as a group of particular military methods, such as intelligence gathering and information infrastructure defense, which can be employed to gain information superiority over potential or actual enemies. Joint Vision 2010 states that in order to facilitate Full Spectrum Dominance,

> We must have information superiority...[which] will require both offensive and defensive information warfare...It will include...nontraditional methods such as electronic intrusion into an information and control network to convince, confuse, or deceive enemy military decision makers...Our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems.[4]

The last of the basic concepts to be presented is Command and Control (C2) doctrine. This area, also a subset of Information Operations, is comprised of many various facets. It is often confusing, since some publications also include Communications (C3), Computers (C4), and Intelligence (C4I), or Warfare (C2W), when discussing specific aspects of command and control functions. The battlespace employment doctrine, which is at the core of all of these sub-categories of C2, is C2W. "C2W is the integrated use of psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions."[5]

Finally, it is important to note that the role that IO plays in the cyber-missions depicted in the new JV 2010, is further developed in several other supporting and related documents. These include the President's National Security Strategy (NSS), the Quadrennial Defense Review (QDR), the CJCS's National Military Strategy (NMS), as well as each of the individual military service concept documents.

These documents, which employ the many diverse tenets of IO, IW, and C2W, form the foundation for future joint military Full Spectrum Dominance operations, including the new concepts of

dominant maneuver, precision engagement, focused logistics, and full-dimension protection, which were previously discussed.

SO WHY THE FUNNY TITLE?

"General! They've Captured Our Hard Drive!" may seem like a funny title for a paper at first glance, but it highlights the fact that future warfare will bring new concerns for military leaders. Furthermore, the following paragraphs will bring to light several key IO issues, which have the potential to negatively impact the total package, previously referred to as Full Spectrum Dominance. The information revolution has provided today's military strategic leaders with a boost to their awesome technological arsenals. These strengths, however, have a potential Achilles' heel, in that there are also inherent weaknesses. Those who practice the strategic art must be prepared to capitalize on Information Operations (IO) advantages, while minimizing the impact of any IO counter-threats seeking to find these weaknesses.

There seems to be two general categories of IO related concerns emerging. These two categories are Technical/Practical, and Political/Cultural. Technical/Practical issues are more familiar (The picture, that the title of this essay paints, is such an issue). The mere fact that the battlefield is becoming

more digitized, puts significant pieces of new American technology physically, as well as virtually, closer to potential enemies. While the military has always had success dealing with physical security, cyber-security is different, new, and dangerous. The National Defense University's "Strategic Assessment 1996" tells us that, "At present, most computer systems are vulnerable to information attacks...the frequency of intrusions is rising, and the possibility of a digital Pearl Harbor cannot be dismissed out of hand."[6] A few examples of these cyber attacks show us a very scary trend.

One such example, occurring about two years ago, involved a story which suddenly broke in most major American newspapers. The news revealed a dramatic hacker attack on the Department of Justice internet homepage. Immediately after the IW attack, Web surfers were welcomed to the cyber-graffiti ridden Department of "In-Justice" homepage, until the network administrators could properly restore the homepage to its original configuration. It was never determined how deeply the Department of Justice networks were invaded, due to their inherent complexity. The hackers responsible for the damage were never found.

Computers, and all their accessories, have now moved out of the isolated, glass encased mainframe rooms of old, and are now everywhere you look, including military aircraft, ships, and tanks. This cyber-proliferation has brought the military world a

new host of problems, merely because military computer targets are so widespread.

Another Technical/Practical issue is described by a renowned information age author, Winn Schwartau. He relates a tale in one of his several recent books, about a military attempt to assess its own information security. A senior level Air Force officer heading up an inspection team, whose mission was to simulate security attacks, was able to remove "one hundred and forty classified diskettes full of military information" from offices at an Air Force Base. He then successfully transported these diskettes by the C2 facility's security guard not once, but twice. The inspector announced to the site's commander shortly thereafter, "I respectfully submit, sir, that your facility has no security. This Air Force Base fails."[7] Today, soldier's field backpacks are being designed to house C2W computers. If military facilities, with constant security forces and other measures in place, cannot properly guard classified computer equipment, then it will be a very challenging task for our men and women in the field to do so. Do our platoon leaders know what to do if their hard drive falls into enemy hands?

Another concern in the IO area, that has significant potential to undermine the Chairman's vision, is the "Year 2000" problem, known as Y2K in high-tech computer jargon. According to an article entitled "The Day the World Shuts Down" in a recent issue of Newsweek magazine, "It [Y2K] represents the ultimate

indignity: the world laid low by two lousy digits...When that date arrives [January 1, 2000], the computers are going to get very confused."[8] The problem is that there is no single military or any other federal agency, which has been provided with the means to develop the ways to ensure that all of the government's computers will continue to operate into the next decade. Two years seems like a long time to prepare, but there is no funding line for Y2K in the budget.

The General Accounting Office (GAO), the watchdog arm of Congress, recently disclosed another Y2K risk area. "...the Social Security Administration (SSA) faces a possible computer crash in the year 2000 because the agency has not started analyzing or fixing several crucial systems affected by the year 2000 software glitch."[9] The worst part is that the Social Security Administration is not the only United States government agency, which has failed to mount a substantial effort to combat the Year 2000 problem. The potentially crippling effect of these and other Y2K repercussions could ripple through many military programs, delaying their fielding schedules, and having significant negative impact on JV 2010 objectives.

Also, it now appears that the huge quantity, coupled with the vast diversity, of different computerized information systems, which are susceptible to a Y2K crash, is a nasty quality all its own. A clear example hit the newspapers a short time ago, revealing the tangled web of airline computer networks, including

air traffic control, flight reservations, airport services, and financial tracking. A USA Today article stated that, "The Federal Aviation Administration is so far behind in its efforts to fix the Year 2000 computer glitch that half the nation's air fleet may have to be grounded during the earliest days, weeks or months of the new millennium, congressional officials say."[10] The strategic implications, including the financial loss, of this many grounded airplanes, are truly significant.

Another concern in this arena, is the practice of computerized information system design, development, and acquisition. Government technology programs have unfortunately been plagued by a history of problems. In an investigative report in 1994 by then Senator, and now Secretary of Defense, William S. Cohen, several significant computer technology deficiencies were highlighted, including:

> Finding 1: The failure of the government to effectively buy needed computer equipment and services has wasted billions of dollars.
>
> Finding 2: Acquisitions of large computer systems are poorly managed and subject to cost overruns and schedule slippages.[11]

Probably the biggest Technical/Practical Information Operations challenge out there for tomorrow's joint military strategic leaders, is the matter of "knowledge fusion and distribution through system integration". The information revolution continues to deliver IW technology improvements at an amazing rate, however service independent acquisitions are

fragmented in funding. Equipment integration across services is in a constant struggle with Pentagon funding methods. "Despite the lip service paid to the ideal of a joint interoperable information system, interoperability is often considered a cost add-on in service acquisition decisions"[12] The risk associated with these Information Warfare support means (separate service funding), ways (acquisition methods), and ends (Full Spectrum Dominance of the battlespace, per Joint Vision 2010) seems to be too high.

One good example of the "interoperability problem", is revealed "between the lines" in the U.S. Army's 1997 Weapon System Handbook. In a discussion of winning the Information War, this handbook states, "As the ground maneuver element of the joint force, the Army needs improved Command, Control, Communications, Computers, and Intelligence (C4I) systems..." Two pages later, it states, "The systems in this book...are part of an integrated approach to make the Army of the future capable of meeting the increased demands of our nation with fewer resources."[13] Although this publication colorfully exhibits the many Army equipment systems of today, there is almost no detail on joint information fusion, or other system integration issues.

In fact, one of the few items, that does attempt such a system integration statement, is the Joint Surveillance Target Attack Radar System (Joint STARS, more commonly JSTARS). This new high-tech system is being fielded jointly with the U.S. Air

Force. The only problem is that only JSTARS terminals can receive JSTARS data, tagging every other system shown in this handbook with an interoperability dilemma. Air Force systems, as one might expect, also have similar JSTARS interoperability problems.

Many of the IO related Technical/Practical issues and examples just described are arguably focused primarily at the tactical, or at the most, the operational level of military command. The problem is that a perception by the American people, that our nation's security is threatened by inferior military equipment and procedures, can quickly be elevated to the strategic level by the press. Actual technical or practical problems, or the mere perception of them by the nation, could create tremendously burdensome oversight and rework. This increased "overhead" could further result in detrimental impacts on our national leaders' ability to convert JV 2010 visions to reality.

INTERNATIONAL INFORMATION WARFARE

The second of the two categories of IO concerns, is the Political/Cultural domain. These issues differ with those previously discussed, since it is not the physical aspects of the information age that are of concern here, but it is the actual existence of practices which invade privacy, or penetrate

national sovereignty, which can lead to national and even international anxiety. This new, challenging, and highly politically sensitive category just might take the lead in strategic importance from its more well known (previously discussed) brother, in the years between now and 2010.

One of the key cultural concerns is that much of this stuff is very new for most senior military leaders. The world is not the neat and clean bipolar environment that it once was during the Cold War. Today's global village is now very volatile, uncertain, chaotic, and ambiguous, making strategic thinking about the present and the future a much tougher ordeal. The very first paragraph of the new joint C2W doctrine even states that, "...the full dimensions of IW policy and its implementations are still emerging."[14] The mere fact that current U.S. military doctrine does not yet provide clear IO understanding, limits leaders' abilities to achieve JV 2010 success.

Another global cultural concern is a growing sense of helplessness, with regard to computer age concepts, in civilian and military sectors. As one author relates, "At one point, if not already, you will be the victim of Information Warfare. If not you, then a member of your family or a close friend. Your company will become a designated target of Information warfare. If not yesterday or today, then definitely tomorrow. You will be hit."[15] Cyber attacks might just become the "polio" of the year 2000 and beyond.

Does the Department of Defense have an institution in place or planned, which can deliver the information technology infrastructure required by current policy documents, such as JV 2010 and the QDR, to provide for proper homeland defense? Unfortunately, the obvious answer is no. In fact, The Report of the President's Commission on Critical Infrastructure Protection, released last October, states that, "To facilitate this new relationship [a new government-private sector partnership to deal with cyber-threats] between government and industry, new mechanisms will be needed, including sector "clearing houses" to provide the focus for industry cooperation and information sharing; a council of CEOs, representatives of state and local government, and Cabinet secretaries to provide policy advice and implementation commitment; a real-time capability for attack warning; and a top-level policy making office in the White House."[16] This statement highlights the fact that today, there is no current person, position, or office in charge of U.S. national cyber-defense.

Another Political/Cultural Information Operations area of concern is a legal one. What sort of IO is legal, and what is not? The answer to this question seems to be a moving target. One problem is that much of our legal system procedures are based on precedent, and revolutionary concepts like Information Warfare and Information Operations are inherently lacking in precedent.

Today's strategic military leaders are forced to examine current legal thinking, and project their best guess into the future. Such guesses involve available frequency ranges for electronic equipment for training and wartime use, the various types of national, commercial, and personal information that can be obtained and stored, and the most appropriate security classification assignment for systems and information stored in those systems.

Strategic leaders must be prepared for the day when legal walls prevent further military advances towards Joint Vision 2010 goals. One example of international legal trauma, was a report of false information. A London Times reporter recently exposed the latest international spy affair, saying that "Israel has set up a panel to investigate an espionage scandal after the disclosure that the country nearly went to war against Syria last year because of disinformation believed by Israeli intelligence"[17] The result of an IW attack like this against the United States could cause irreparable damage.

The final Information Operations issue of this type to be discussed will be one of recent intense political disdain. Although international spying and intelligence collection has existed for many years, the USA's open IO display has many countries, such as Russia and China, worried. "...the ubiquity of global communications is creating new avenues for the interests, culture, and values of the United States to percolate

overseas...the existence of these channels makes it easier for the United states government to go over the heads of other governments and communicate directly to their citizens."[18] Billboards advertising American products, which can be seen easily from Red Square, are one thing. Massive quantities of U.S. capitalism swarming the global internet, are quite another. In fact, English is the default internet language.

These countries see this American IO arrogance as a direct threat to their sovereignty. International diplomatic, financial, and trade relations could be severely strained if future leaders do not put us on the proper strategic course. In fact, this issue alone could provide the most significant negative impact to JV 2010 becoming a reality, since it is this vision of dominance which is inherently disturbing to these countries.

JEWELS IN THE ROUGH

Numerous challenges clearly exist, with respect to the chances of attaining the lofty goals envisioned by the Chairman of the Joint Chiefs of Staff. There are, however, several "jewels in the rough". Military and corporate sectors have produced a few very encouraging examples of organizations, that are directly contributing to meeting the JV 2010 challenge.

Several of these jewels are presented, not as models of perfection, but rather as a few guiding lights for the rest of us to follow during these often very foggy days.

A good question to highlight a first example, might be, "How does the military go about getting sufficient IW resources to support modern joint warfare?". Although the answer is usually a stuttered, "It depends...", all the services have a separate, but similar approach. For example, "The Marine Corps maintains a robust but focused Science and Technology (S&T) Program to assess and develop the entire spectrum of technologies...to harness the technology needed to provide the FMF [Fleet Marine Force] with the capabilities to perform those specified and implied missions assigned by law".[19] The S&T Program Managers comply with their tasking, which directs joint force integration, and highly encourages joint acquisition of equipment and weapon systems.

Another shining star in the information revolution galaxy is the newly formed Joint Command and Control Warfare Center (JC2WC), which serves many vital IW support roles, including "direct command and control warfare support to operational commanders,...interface with the Joint Staff, Services, DOD and non-DOD agencies to integrate IW,...[and to] coordinate with the services on C2W engineering initiatives, laboratory programs, and industrial developments."[20] This joint venture appears to be filling the system interoperability void earlier discussed. There is a big void, but this is a genuinely impressive step in the right direction.

A final gleam of hope is being provided by the great American software engineering industry. Although they are the culprits in our Year 2000 dilemma, many programmers are attempting to recover as gracefully as possible. Several of these kinds of examples exist today, but one recently reported on in a popular computer trade magazine, showed that "Platinum Technologies Inc.'s latest [Y2K] testing tool uses business rules to automatically "age" data in a company's database [or government agency's database] and then uses that data to check for year 2000 compliance."[21] These new software tools aimed at tackling the Y2K challenge just might be more of a salvation than anyone now knows.

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

In conclusion, there are several strategic level Information Operations (IO) concerns, which may impact the goal of Full Spectrum Dominance, as described in JV 2010, and related documents. The strategic road to IO support for Joint Vision 2010 is fraught with many potential pitfalls. Although the recent victories in the Cold War and the War in the Gulf were significantly influenced by superior IW and C2W support, many areas of improvement are needed, and remain unresolved. The goals of the Chairman of the Joint Chiefs of Staff are visionary, but Full Spectrum Dominance, as described in this vision, is NOT GOING TO HAPPEN ON TIME. When the year 2010 arrives, we may be

making great progress towards the goal, but current and potential enemies will be making progress as well!

One recommendation to accelerate such progress, is that there should be a continuous effort on assessment. It will be difficult enough in this often confusing, and always complex environment, for strategic leaders to move towards and carry out the missions depicted in JV 2010. Some excellent guidance in the area of information technology support, according to Secretary (then Senator) Cohen in his 1994 investigative report include:

1) Emphasize early oversight and planning [on information system acquisitions].
2) Reduce bureaucratic barriers to purchases.
3) Size [automation related] projects to manageable levels.
4) Encourage innovation.
5) Create incentives for the government and contractors to perform.
6) Communicate lessons learned.
7) Reevaluate existing procurements and [if required] halt new procurements until the computer acquisition process is improved.[22]

Some would argue that many of these items are being done, especially in the area of computerized information system development. Many others, including this author, while agreeing that some of the above ideas are being put in motion, can quickly point to significant deficiencies. In addition, to those areas listed above, every strategic military leader needs to get operational, and maybe even a bit tactical, to help beat the Y2K bug. Since units get no special funding, this is a tough nut to crack, especially if the preferred method of professional analysts is used. They may be expensive now, but the sooner a

unit can get out from under this rock, the better. The issues just described could definitely and significantly degrade or delay the United States Military's ability to achieve the Chairman's vision.

Probably the biggest single action, that the strategic leaders of this country could undertake, would be to PUT SOMEONE IN CHARGE. If the President of the United States were to ask today, "Who is my Chief Information Officer?" (every major corporation has one of these CIO's), there would most likely be lots of finger pointing, but no real answer. The problem is that too many folks have their piece of the action, but there is no single government entity at the top. It is about time to take a lesson from corporate America, and the President's Commission on Critical Infrastructure Protection, and put someone in a truly powerful and responsible position to get us to Joint Vision 2010. Without this kind of focus and leadership to keep us on the true part of the path, the ride will just be too bumpy, and the jeep will break down.

Finally, it is the hope of this author, that in some small way, the ideas and concepts presented here will provide some food for strategic thought, in the realm of current and future Information Operations. Remember that these concepts are all moving targets. The world is no longer bi-polar, but rather quite chaotic and volatile.

One of this planets' greatest strategic leaders, Attila the Hun, warns us, "Do not understimate the power of an enemy, no matter how great or small, to rise against you another day." [23]

Its an information jungle out there, with cyber-threats large and small. Keep Charging!

Word count 4645.

ENDNOTES

[1] Joint Staff, Joint Vision 2010, Washington DC, 1,2.

[2] Department of Defense, Information Operations (IO), Defense Directive S-3600.1 (Washington, DC: U.S. Department of Defense, 9 December 1996), 1-1.

[3] Ibid.

[4] Joint Staff, Joint Vision 2010, Washington DC, 16.

[4] Joint Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Publication 3-13.1, February 7, 1996, v.

[6] National Defense University, Institute for National Strategic Studies, Strategic Assessment 1996: Instruments of U.S. Power, (Washington, DC: National Defense University Press, 1996), 197.

[7] Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (New York, NY: Thunder's Mouth Press, 1994), 254.

[8] Newsweek, "The Day the World Shuts Down", June 2, 1997, 54.

[9] Rajiv Chandrasekaran, "Social Security Gets Year 2000 Warning: More Work Needed on Glitch, GAO says", The Washington Post, 5 November 1997.

[10] M.J. Zuckerman, "Glitch may stop 50% of flights", USA Today, 4 February 1998.

[11] Cohen, Senator William S., Computer Chaos: Billions Wasted Buying Federal Computer Systems, October 12, 1994, 3 and 7.

[12] National Defense University Institute for National Strategic Studies, Strategic Assessment 1996: Instruments of U.S. Power, 190.

[13] U.S. Army, Weapon Systems: United States Army 1997, (Washington DC: Department of the Army), 5,7.

[14] Joint staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Publication 3-13.1, February 7, 1996, i.

[15] Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (New York, NY: Thunder's Mouth Press, 1994), 11.

[16] President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, (Washington DC, October 1997), xi.

[17] Christopher Walker, "False Spy Reports Pushed Israel to Brink of War", London Times, 5 December 1997.

[18] National Defense University, Institute for National Strategic Studies, Strategic Assessment 1996: Instruments of U.S. Power, (Washington, DC: National Defense University Press, 1996), 5.

[19] U.S. Marine Corps, Concepts & Issues 97 "Making Marines, Winning Battles", (Washington DC, 1997), 44.

[20] Joint staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Publication 3-13.1, February 7, 1996, B-A-1,2.

[21] Antoine Gonsalves, "Data 'Aging' Speeds Y2K Work", PC Week, 19 January 1998, 39.

[22] Cohen, Senator William S., Computer Chaos: Billions Wasted Buying Federal Computer Systems, October 12, 1994, 28 and 29.

[23] Wess Roberts, Leadership Secrets of Attila the Hun (New York, NY: Warner Books Inc., 1987), 57.

BIBLIOGRAPHY

Bade, William B., The Survivor's Guide to Library Research. New York, N.Y.: Zondervan's, 1990.

Campen, Alan D., The First Information War. Fairfax, VA: AFCEA International Press, 1992.

Chandrasekaran, Rajiv, "Social Security Gets Year 2000 Warning: More Work Needed on Glitch, GAO says", The Washington Post, 5 November 1997.

Cohen, Senator William S., Computer Chaos: Billions Wasted Buying Federal Computer Systems, Washington, D.C., 1994.

Department of the Army, Weapon Systems: United States Army 1997, Washington D.C., 1997.

Department of Defense, Information Operations (IO), Defense Directive S-3600.1. Washington, D.C.: U.S. Department of Defense, 9 December 1996.

Department of the Navy, U.S. Marine Corps, Concepts & Issues 97 "Making Marines, Winning Battles", Washington D.C., 1997.

Gonsalves, Antoine, "Data 'Aging' Speeds Y2K Work", PC Week, 19 January 1998

Joint Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Publication 3-13.1. Washington, D.C.: U.S. Joint Staff, 1996.

Joint Staff, Joint Vision 2010. Washington, D.C.: U.S. Joint Staff, 1997.

National Defense University, Institute for National Strategic Studies, Strategic Assessment 1996: Instruments of U.S. Power. Washington, D.C.: National Defense University Press, 1996.

Peterson, John L., The Road to 2015. Corte Madera, CA: Waite Group, 1994.

President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures. Washington, D.C., 1997.

Roberts, Wess, Leadership Secrets of Attila the Hun. New York, NY: Warner Books Inc., 1987.

Schwartau, Winn, Information Warfare: Chaos on the Electronic Superhighway. New York, NY: Thunder's Mouth Press, 1994.

Walker, Christopher. "False Spy Reports Pushed Israel to Brink of War", London Times, 5 December 1997.

Zuckerman, M. J. "Glitch may stop 50% of flights", USA Today, 4 February 1998.